

CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. A method of conducting business electronically between a first party and a
5 second party, comprising:

providing a third party who knows an identity of the first party but no
privacy-compromising information regarding a proposed electronic business
transaction between the first and second parties; and

conducting the electronic business transaction between said first and
second parties through the third party such that said identity of said first party is
kept from the second party.

2. A method of performing electronic commerce without a candidate customer
being forced to disclose private data together with an identity of the candidate
15 customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the
candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can
be identified as a legitimate owner of the item without revealing the identity of

20 said customer; and
YO999-486

009250-74732560

Sub
95

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity.

5 3. The method according to claim 2, wherein the customer establishes the relationship with the third party which serves for all further engagements with business entities.

10 4. The method according to claim 2, wherein a Fourth Party delivers to the customer a portable device P(C) which carries biometrics of the customer such that the customer can be identified as a legitimate owner of the portable device P(C) without revealing the identity of said customer.

5. The method according to claim 4, wherein the device P(C) delivers a number S(C) at each transaction, and the number S(C) is readable from the portable device P(C) only in the presence of the customer.

15 6. The method according to claim 5, wherein said portable device P(C) generates numbers $S(C,n)$, where n is an integer belonging to a set $\{1, 2, \dots, N\}$, and wherein for at least one of each new business unit and other partner of the customer, a new number n is chosen for all further transaction between the customer and said at least one of each new business unit and other partner.

YO999-486

00999-486

AS
Cont'd

Sub
A6

7. The method according to claim 2, wherein the business entity chooses a set of verifiers $V_j, j = 1, 2, \dots, N,$,

wherein said verifiers are each equipped to verify portable devices, and are connectable to a network so as to output information to the third party T using privacy protection.

8. The method according to claim 2, wherein when deciding to register with a business entity, the customer sends to the third party an application and a software to encrypt the application using a public key $pu1(I)$ where $(Pr1(I), pu1(I))$ is a public signature scheme of the business entity,

said software further allowing the customer to compute a public signature scheme $(Pr2(I,C), pu2(I,C))$, said application being provided over a network connected to said business entity.

9. The method according to claim 8, wherein the application has a header having identification data about the customer written together with a number $S(C)$

associated with the proprietary item, and a body where personal or other data associated with said customer and $pu2(I,C)$ are written after encryption using $pu1(I)$.

10. The method according to claim 9, wherein when receiving the application, the third party replaces the header with a number $N(T,C,I)$ which is sent to insurance

Ab
Contd

009250-74732500

entity with body of the completed application, wherein said business entity
decrypts body and decides on an offer price if any, and

wherein a decision is communicated to the business entity after encryption
using $pu2(I,C)$ together with $N(T,C,I)$, and the business entity forwards
5 $pu2(I,C)(D)$ to the customer.

11. The method according to claim 2, wherein, before sending application to the
business entity, the customer accesses one or more verifiers V_j , and wherein the
customer identifies itself to each verifier V_j using a number $S(C)$ associated with
the proprietary item, and requests V_j to send $S(C)$ to the business entity, together
10 with data verified by V_j .

~~12. The method according to claim 11, wherein communication to the business
entity is performed by appending to the number $S(C)$ the relevant data encrypted
using $pu1(I)$~~

13. The method according to claim 11, wherein a link between the third party
15 and the business entity is provided by the third party posting all completed
applications on a dedicated world-wide-web (WWW) page after removing clear
identification thereof, and tagging by a number $N(T,C, I)$ which has a redundancy
allowing the business entity, but no other party, to recognize this number as a
number associated with the business entity.

YO999-486

009250-74732560

Sub
B3

14. The method according to claim 2, wherein a payment between a business entity and a third party is documented by the paying party by attaching a tagging number to the payment,

said tagging number being communicated to a bank of the paying party, and accompanies the transaction order to the bank of the payee, and

wherein the paying bank accepts the money transfer in exchange of the tag coded using a private key of the payee's bank.

15. The method according to claim 2, wherein, with a relationship between the customer and the business entity previously established, the business entity interacts with the customer despite not knowing an identity of customer.

16. The method according to claim 15, wherein, when submitting a transaction request, the customer addresses the transaction request to the third party, after selectively consulting with one or more verifiers Vj.

17. The method according to claim 16, wherein, after processing the transaction request, the business entity sends a communication encrypted using a public key $pu2(I,C)$, to the third party, and said third party transmits the encrypted communication to the customer.

18. The method according to claim 17, wherein said communication includes one of a payment, a request for further data, and a declination of the transaction request.

19. The method according to claim 2, further comprising selecting a purveyor of
5 good or services as the business entity.

20. The method according to claim 2, wherein the proprietary item comprises a device $P(C)$ which delivers a number $S(C)$ at each transaction, and the number $S(C)$ is readable from the device $P(C)$ only under authorization from the customer.

10 21. The method according to claim 2, wherein the business entity chooses a set of verifiers V_j , where $j = 1, 2, \dots, N$.

22. The method according to claim 2, wherein said item carries biometrics of the customer.

23. The method according to claim 2, wherein said third party receives the
15 identity of the customer, and said business entity receives information other than the identity of the customer.

24. A method of selecting a purveyor of goods or services in a confidential manner over a network, comprising:

5 sending, by a customer, an application to a third party, wherein said application is taken electronically from a business entity, along with a code which allows encrypting the application using a public key $pu1(I)$, where $(Pr1(I), pu1(I))$ is a public signature scheme of business entity, said code allowing the customer to compute a public signature scheme $(Pr2(I,C), pu2(I,C))$.

10 25. The method according to claim 24, wherein the application includes a header where identification data about the customer is written together with a number $S(C)$, and a body where other data of the customer and the key $pu2(I,C)$ is written after encryption using the public key $pu1(I)$.

26. The method according to claim 25, wherein when receiving the application, the third party replaces the header with a number $N(T,C,I)$ which is sent to the business entity with the completed body of the application.

15 27. The method according to claim 26, wherein the business entity decrypts the body using $Pr1(I)(pu1(DATA))$ and makes a decision D on whether to proceed and if so, an offer price, and

 wherein the decision D is communicated to the third party after encryption using public key $pu2(I,C)$ together with the number $N(T,C,I)$, and
YO999-486

009250-72732560

Sub
A8

A B

wherein the third party, using the number $N(T,C,I)$ to recognize the customer, sends the public key $pu2(I,C)(D)$ to the customer, who decrypts using a private key $Pr2(I,C)$ to obtain

$$D = Pr2(I,C)(pu2(I,C)(D)).$$

5 28. The method according to claim 24, wherein before sending application to the business entity, the customer accesses one or more verifiers.

29. The method according to claim 24, further comprising:

establishing a customer-purveyor contact over the network.

30. The method according to claim 29, wherein said establishing comprises:

10 when submitting a transaction request, encrypted using $pi1(I)$, the customer addresses the request to the third party, after selectively accessing one or more verifiers V_j ;

transmitting, by the third party T , the transaction request to the business entity after removing a header and attaching a number

15 $N_{transaction}(T,C,I,Transaction)$ thereto; and

processing the request by the business entity.

31. The method according to claim 30, wherein said establishing further comprises:

YO999-486

009250-74782500

sending, by the business entity, a communication to the third party.

32. The method according to claim 31, said establishing further comprising:

transmitting said communication, after or while processing the transaction request, to the third party, said request being encrypted using the public key

5 pu2(I,C); and

transmitting, by the third party, the communication to the customer.

33. The method according to claim 31, wherein the communication includes one of a payment, a request for further data, and a declination of part or all of the transaction.

10 34. A system for conducting business electronically between a first party and a second party, comprising:

means for providing to a third party an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties; and

15 means for conducting the electronic business transaction between said first and second parties through the third party such that said identity of said first party is kept from the second party.

5 providing to a third party an identity of the first party but no
privacy-compromising information regarding a proposed electronic business
transaction between the first and second parties; and

10

15

15

20

20

37. A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity.